CA Nimsoft Monitor para Flow Analysis

Guia do Usuário

Release 1.0

Histórico da revisão do documento

Versão do documento	Data	Alterações
1.0	9/10/2012	Guia do Usuário da Versão Inicial do *CA Nimsoft Monitor para Flow Analysis*

Entrar em contato com a Nimsoft

Para sua conveniência, a Nimsoft fornece um único site onde é possível acessar as informações sobre os produtos da Nimsoft.

No endereço http://support.nimsoft.com/, é possível acessar o seguinte:

- Informações para contato online e telefônico, assistência técnica e atendimento ao cliente
- Informações sobre fóruns e comunidades de usuário
- Downloads de produto e documentação
- Políticas e diretrizes de suporte da Nimsoft
- Outros recursos úteis adequados ao seu produto

Fazer comentários

Caso tenha algum comentário ou pergunta sobre a documentação de produtos da Nimsoft, envie uma mensagem para support@nimsoft.com.

Avisos legais

Garantia

O material contido neste documento é fornecido "como está" e está sujeito a alterações em edições futuras sem aviso prévio. Além disso, na medida permitida pela lei aplicável, a Nimsoft LLC isenta-se de todas as garantias, sejam implícitas ou expressas, com relação a este manual e todas as informações contidas no presente documento, incluindo, sem limitação, garantias implícitas de comerciabilidade e adequação para um determinado fim. A Nimsoft LLC não será responsabilizada por erros ou danos acidentais ou resultantes do fornecimento, uso ou desempenho deste documento ou de qualquer outra informação contida no presente. Caso a Nimsoft LLC e o usuário tenham um acordo por escrito à parte sobre termos de garantia que cobrem o material deste documento conflitando com estes termos, os termos de garantia do acordo à parte prevalecerão.

Licenças de tecnologia

O hardware e/ou software descritos neste documento são fornecidos sob uma licença e poderão ser usados ou copiados somente de acordo com os termos da referida licença.

Nenhuma parte deste manual poderá ser reproduzida de qualquer forma ou por qualquer meio (incluindo a recuperação e o armazenamento eletrônico ou a tradução em um idioma estrangeiro) sem um acordo prévio e consentimento por escrito da Nimsoft LLC, em conformidade com as leis de direitos autorais internacional e dos EUA.

Legenda de direitos restritos

Se o uso do software for destinado ao cumprimento de um contrato ou subcontrato do governo dos Estados Unidos da América -EUA, o software será fornecido e licenciado como "software comercial para computadores", conforme definido no DFAR 252.227-7014 (junho de 1995), ou como um "item comercial", conforme definido no FAR 2.101(a); ou como "software de computador restrito", conforme definido no FAR 52.227-19 (junho de 1987) ou em qualquer regulamento equivalente do órgão ou Cláusula contratual. O uso, a duplicação ou a divulgação do software está sujeito aos termos de licença comercial padrão da Nimsoft LLC, os departamentos que não fazem parte do DOD (Department of Defense) e os órgãos do governo dos EUA não receberão mais Direitos do que os Direitos Restritos, conforme definido no FAR 52.227-19(c)(1-2) (junho de 1987). Os usuários do governo dos EUA não receberão mais que Direitos Limitados, conforme definido no FAR 52.227-14 (junho de 1987) ou no DFAR 252.227-7015 (b)(2) (novembro de 1995), conforme aplicável em quaisquer dados técnicos.

Marcas registradas

Nimsoft é uma marca registrada da CA.

Adobe®, Acrobat®, Acrobat Reader® e Acrobat Exchange® são marcas registradas da Adobe Systems Incorporated.

Intel® e Pentium® são marcas registradas da Intel Corporation dos EUA.

Java(TM) é uma marca registrada da Sun Microsystems, Inc. dos EUA.

Microsoft® e Windows® são marcas registradas da Microsoft Corporation dos EUA.

Netscape(TM) é uma marca registrada da Netscape Communications Corporation dos EUA.

Oracle® é uma marca registrada da Oracle Corporation, Redwood City, Califórnia, Estados Unidos.

UNIX® é uma marca registrada do Open Group.

ITIL® é uma marca comercial registrada do Office of Government Commerce no Reino Unido e em outros países.

Todas as marcas comerciais, nomes comerciais, marcas de serviços e logotipos mencionados neste documento pertencem às respectivas empresas.

Índice

Capítulo 1: Introdução

Sobre este guia

Este guia o ajuda a obter o máximo benefício do Nimsoft Monitor para a solução do Flow Analysis. O guia contém as seguintes seções:

- **Introdução** -- Informações sobre este guia e uma introdução aos conceitos do Flow Analysis
- **Guia rápido** -- Abrange as etapas necessárias para iniciar o uso do Flow Analysis
  - Componentes de pré-requisito
  - Configurar o portlet Gerador de relatórios
  - Configuração -- Abrange as tarefas de configuração necessárias para:
    - acesso de porta e roteadores que fornecem fluxo de dados da rede
    - o probe do Flow Analysis e o sistema do coletor
    - o portlet e a interface gráfica do usuário (GUI) do Flow Analysis
- **Relatórios** -- descreve a interface gráfica do usuário do Flow Analysis, seus controles, e os relatórios de fluxo de dados que estão disponíveis
- **Solução de problemas** -- descreve problemas do uso do produto e suas soluções.

Conceitos do Flow Analysis

O Flow Analysis foi desenvolvido para integrar a exibição do fluxo de tráfego através da rede com os dados e alarmes de QoS, todos exibidos no Nimsoft Unified Management Portal (UMP). Com o Flow Analysis, você pode:

- Identificar imediatamente as interfaces, hosts e os aplicativos que geram a maior parte do tráfego em sua empresa. Essa informação é essencial para a solução de problemas de curto e longo prazo.
- Revisar os alarmes do Nimsoft, juntamente com o fluxo de dados para identificar os problemas de rede de forma rápida.
- Analisar tendências em aplicativos, hosts e conversas por classe de serviço. Essas informações ajudam você a otimizar a infraestrutura de rede para o desempenho do aplicativo.

Terminologia do Flow Analysis

Netflow

NetFlow refere-se aos protocolos (NetFlow versões 5, 7 e 9, bem como IPFIX, Jflow, sFlow, cflowd, Rflow e NetStream). que ativam a coleta de estatísticas de tráfego IP nas interfaces do dispositivo de rede. Um roteador está configurado para exportar informações do fluxo de dados, envio de pacotes UDP que contêm estatísticas de fluxo para um coletor.

O fluxo de informações é útil para responder aos seguintes tipos de perguntas:

- Você sabe quais são todos os aplicativos em execução na sua rede?
- Quais são os padrões de tráfego de aplicativos?
- Quais aplicativos e hosts estão consumindo a maior parte da largura de banda?
- Qual a capacidade de link que preciso no futuro? Realmente a resposta aos problemas de desempenho é maior largura de banda?

Conversa

A conversa é uma sessão de tráfego entre sub-redes ou entre usuários (entre hosts). O portal do Flow Analysis exibe esta informação -- É possível descobrir se uma determinada conversa está causando um pico de tráfego em uma interface, por exemplo, e identifica as principais conversas com base no volume.

Fluxo

Um fluxo é um conjunto de pacotes IP que passam em um ponto de observação de rede durante um certo intervalo de tempo. Um fluxo pode consistir em Flexible NetFlow, Sampled NetFlow, NetFlow v5, v7, ou v9; sFlow versão 5 ou quaisquer versões comparáveis do IPFIX, Jflow, cFlow ou NetStream.

Interface

Uma interface é um ponto de conexão, como uma interface serial, Frame Relay, Fast Ethernet, ATM ou PVC. O Flow Analysis informa sobre qualquer interface lógica ativa em um roteador suportado que tem seu fluxo ativo. O portal exibe as interfaces que são monitoradas no seu ambiente.

Protocolo

Um protocolo é um padrão para controlar a comunicação entre computadores. Os protocolos comuns incluem: HTTP, SNMP, FTP e VoIP. As informações exibidas podem incluir os principais protocolos de entrada e saída de determinada interface. Estas informações podem ajudar a identificar qual aplicativo está gerando tráfego de rede. Também é possível criar e executar relatórios a fim de determinar quais protocolos e aplicativos são usados por grupos diferentes em sua empresa.

QoS (Qualidade de serviço)

QoS (Qualidade de serviço) é um nível definido de desempenho -- qualidade de transmissão e disponibilidade do serviço -- em uma rede de dados.

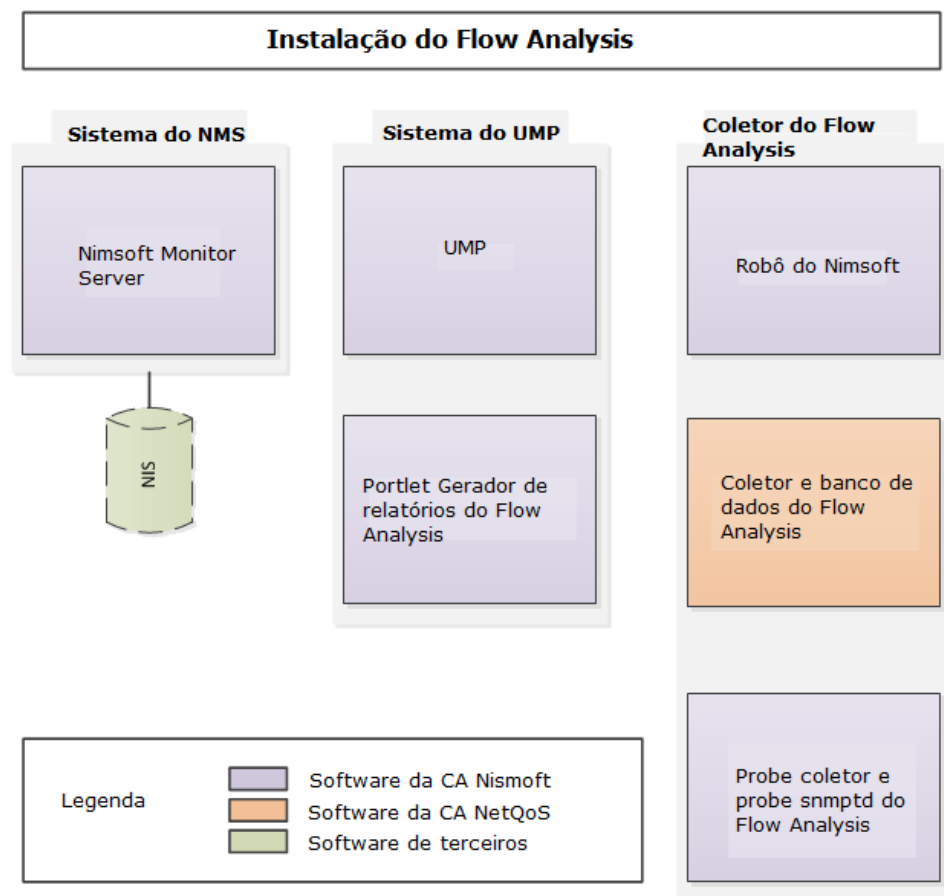
Relatório

Um relatório é uma exibição dos dados coletados, que é possível ser visualizado no portlet do Flow Analysis no UMP. É possível exportar relatórios como arquivos de valores separados por vírgulas (CSV).

Capítulo 2: Introdução

Esta seção contém os seguintes tópicos:

Pré-requisitos

Consulte o *Guia de Instalação do Flow Analysis* e confirme se todos os componentes de software necessários estão instalados, licenciados e operacionais:

- Nimsoft Monitor Server e o banco de dados do NIS
- Unified Monitoring Portal (UMP) e o portlet Gerador de relatórios do Flow Analysis
- O coletor e o banco de dados do Flow Analysis, um robô do Nimsoft e o probe coletor e o probe snmptd do Flow Analysis.

Observação: o coletor e o banco de dados do Flow Analysis são baseados nos produtos CA NetQoS Harvester e Reporter/Analyzer, respectivamente.

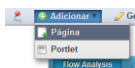
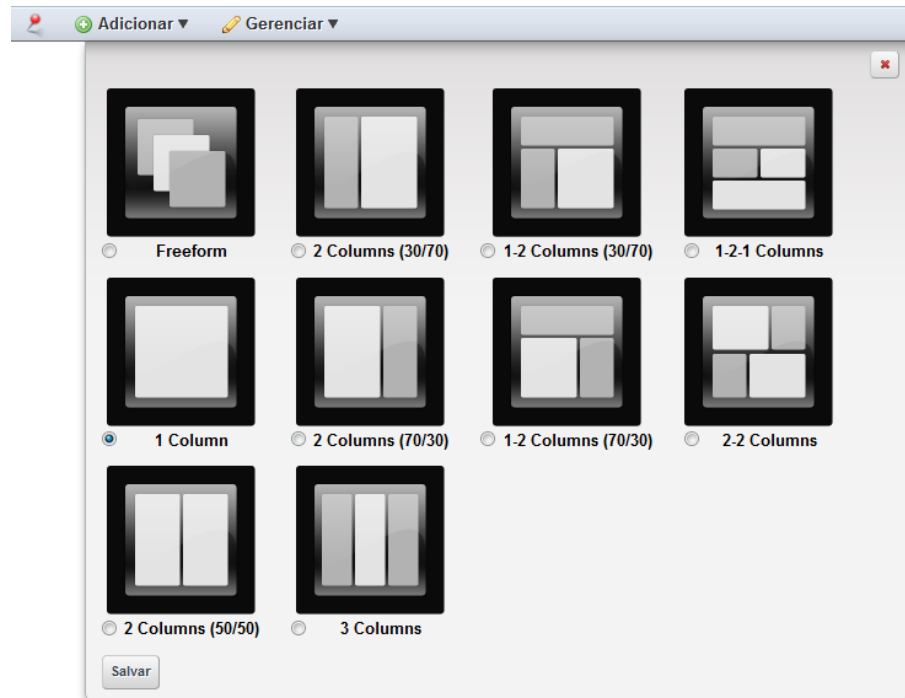
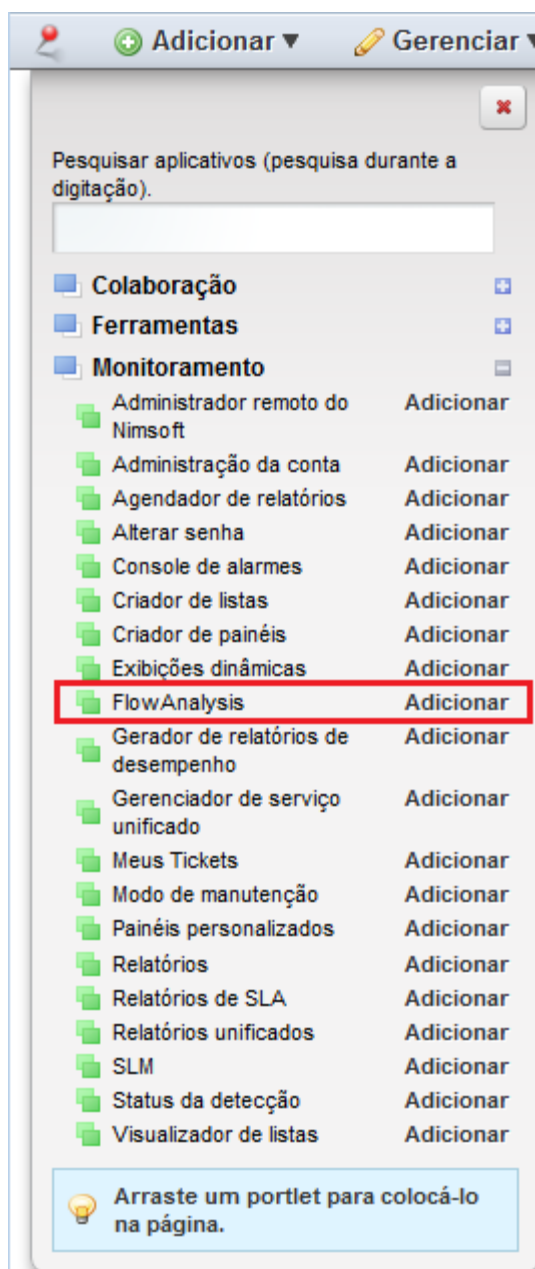
Implantar o portlet Gerador de relatórios do Flow Analysis

Para configurar os componentes do Flow Analysis e visualizar os relatórios de fluxo de dados, o portlet Gerador de relatórios do Flow Analysis precisa ser implantado dentro do Unified Monitoring Portal (UMP).

Para começar, siga estas etapas:

1. Confirme se o probe ump_flow foi implantado no robô do sistema UMP. Isso pode ser verificado no Gerenciador de infraestrutura. Localize o ícone do robô do sistema UMP e o ícone do probe ump_flow deve estar visível sob ele e na cor verde. Para revisar as instruções de instalação, consulte a seção Instalação do portlet Gerador de relatórios do Flow Analysis no *Guia de Instalação do Flow Analysis*).
2. Inicie o UMP (http://<IPaddress_of_UMP_system>)
3. Siga as etapas abaixo para adicionar a guia do Flow Analysis para o UMP.

   Observação: um tratamento mais completo de como configurar páginas e portais no UMP está disponível na ajuda online do UMP na seção **Bem-vindo> Introdução ao UMP**.

   1. Adicionar uma página vazia: na parte superior esquerda do UMP, escolha: **Adicionar > Página**, atribua um nome para a nova página (recomendamos Flow Analysis) e, em seguida, clique na caixa de seleção para confirmar e salvar.

2. Ajustar o layout da página: selecione a nova página e, em seguida, selecione **Gerenciar> Layout de Página> 1 coluna** no menu na parte superior esquerda da janela do navegador e clique em **Salvar**.

3. Instalar o portlet do Flow Analysis na nova página: escolha **Adicionar> Portlet**. Em seguida, selecione o Flow Analysis em **Monitoramento** e clique em **Adicionar**.

4. O portlet é carregado na página, inicia e encontra os coletores do Flow Analysis disponíveis. Aqueles que são localizados são exibidos na lista suspensa do Coletor no formulário "hub/robô/domínio".

Observação: o probe discovery_server deve ser executado no host do NMS para a lista suspensa do coletor exibir os coletores do Flow Analysis. Se um coletor existente não está listado nesse menu suspenso, talvez ele não tenha sido detectado ainda. O reinício dos probes discovery_server e discovery_agent causará a detecção ao executar novamente e localizar outros coletores.

5. Selecione o coletor desejado a partir da lista suspensa.
6. A página principal do Flow Analysis exibe estes três gráficos dos dados do relatório TopN:
    1. Interfaces principais
    2. Hosts principais
    3. Aplicativos principais.

Observação: se você tiver acabado de iniciar o sistema, os dados não poderão ser exibidos até que um intervalo de quinze minutos tenha passado.

É possível detalhar os dados exibidos clicando-se nos links em azul. Consulte a seção sobre Página principal do Flow Analysis (na página 30) para obter detalhes.

Configuração

A configuração do Flow Analysis consiste nas seguintes tarefas:

Configurando o Flow Analysis

Administrador do servidor

Sistema Coletor

Abrir a porta 9995 (UDP)

Dispositivos de rede

Ativar dados de fluxo em interfaces

GUI de configuração do Flow Analysis

Configurar probe do Flow Analysis

Configurar coletor (Harvester de NetQoS)

Configurar relatórios

Legenda

Software da CA Nimsoft

Software da CA NetQoS

Software de terceiros

Um administrador do sistema com o conhecimento do Windows Server 2008 e direitos administrativos nos hosts executa essas etapas de configuração:

1. Abrir a porta 9995 ao tráfego UDP no sistema do coletor do Flow Analysis
2. Ativar o NetFlow (ou outro protocolo de monitoramento de fluxo) na interface do dispositivo de rede como o desejado (um administrador de rede com o acesso administrativo a esses dispositivos pode ser necessário para executar esta etapa)
3. Configurar o probe do Flow Analysis
4. Configurar o coletor do Flow Analysis
5. Configurar relatórios.

Abrir a porta 9995 (UDP)

Abrir a porta 9995 ao tráfego UDP no sistema do coletor. Confirmar se o tráfego UDP pode passar entre seus dispositivos de rede e o host do coletor que está usando esta porta.

Dispositivos de rede

Para ativar o NetFlow em roteadores compatíveis com o NetFlow, execute as seguintes etapas em cada roteador com suporte para versões 5, 7 e 9 do NetFlow.

Observação: antes de começar, colete as informações a seguir para cada roteador que desejar monitorar:

- Endereço de origem
- Sequência de caracteres da comunidade de leitura SNMP
- Versão do NetFlow (se aplicável)

Protocolos de fluxo compatíveis:

- NetFlow v5, v7 e v9
- sFlow versão 5
- IPFIX, Jflow, cFlow e NetStream padrões e em conformidade com os padrões para o NetFlow v5, v7 ou v9

Siga estas etapas:

1. Salve uma cópia de backup das configurações atuais para um servidor TFTP (Trivial File Transfer Protocol - Protocolo de transferência de arquivo simples) ou para a área de trabalho.
2. Execute o comando **copy run start** ou **wr mem** antes de fazer quaisquer alterações nos roteadores que deseja monitorar.

   A execução deste comando ajuda a garantir que todas as configurações atuais serão salvas na memória estática caso o roteador bloqueie ou reinicie.
3. Configure a exportação do NetFlow inserindo os seguintes comandos IOS na ordem mostrada:

   ```
   ip flow-export version <version_number>
   ip flow-export source <interface>
   ip flow-export destination <IP address of the installation system>
   9995
   ip flow-cache timeout active 1
   ```

   Observação: para o segundo comando na série, o endereço IP da interface de origem pode ser alterado. A Cisco recomenda que você configure uma interface de origem loopback para usar.

4. Para cada interface lógica, vá para a interface e digite:
   `ip route-cache flow`

   ou

   `ip flow ingress (para versões mais recentes do IOS)`

5. Configure a persistência do índice em cada roteador usando o seguinte comando:
   `config# snmp-server ifindex persist`

   Observação: os Roteadores da Cisco das famílias das séries 7200, 7500 e 12000 GSR suportam a persistência de índice.

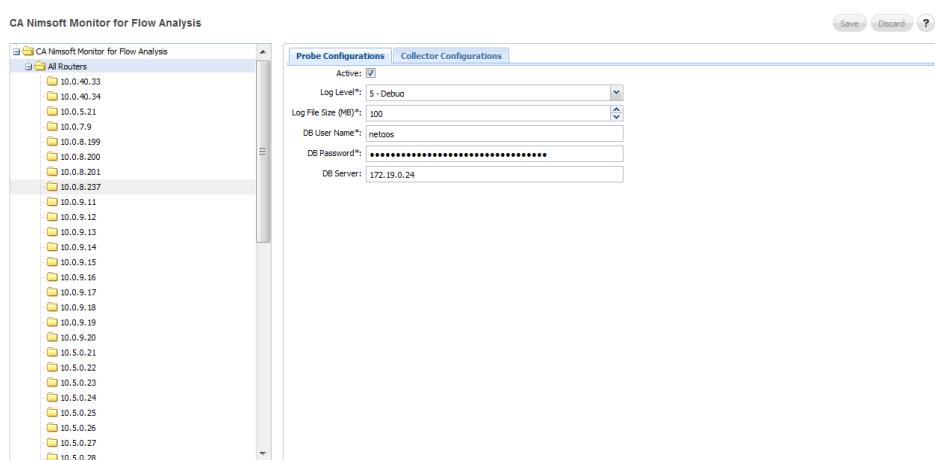
6. Verifique se você possui um Sup II ou mecanismo de supervisão superior, se você usar os switches Catalyst 6500 e 7600.

   Observação: para outros comandos de switch Catalyst 6500 e 7600, consulte a documentação de comandos do NetFlow da Cisco.

Verifique se os dados do fluxo estão sendo recebidos

No sistema do coletor (onde o componente do software de banco de dados do Flow Analysis está instalado), vá para o diretório D:\NETQOS\Netflow\datafiles\HarvesterWork. Deve haver muitos arquivos neste diretório chamado <numeric_value>-9995.tbn.inc. Pode haver mais arquivos com o mesmo esquema de nomenclatura com uma extensão de arquivo .tmp. Se você visualizar arquivos <numeric_value> -9995.tbn.inc que são maiores que 0 KB, isso indica que o fluxo de dados está sendo recebido.

Abrindo a interface gráfica do usuário (GUI) de configuração

Clique no botão **Configurar** na parte superior direita da GUI do Flow Analysis no UMP para abrir a interface gráfica de configuração em uma janela separada:

Quando a interface do usuário de configuração é iniciada pela primeira vez, não existe nenhum dado no quadro do lado esquerdo a ser exibido até que um coletor esteja ativado. Com um Coletor ativado, uma hierarquia de dispositivos de rede é exibida.

No quadro direito, há duas guias, **Configurações de probe** e **Configurações do coletor**, as quais controlam as configurações para o probe e coletor do Flow Analysis, respectivamente.

Configurar o probe do Flow Analysis

A guia Configurações do probe na interface gráfica de usuário de configuração do Flow Analysis permite definir e alterar estes atributos:

Atributo	Tipo	Observações
DB Server	Endereço IP	IP do banco de dados do Flow Analysis
Nome de usuário de DB	sequência de caracteres	nome de usuário para o banco de dados do Flow Analysis; padrão = "netqos"
Senha DB	sequência de caracteres	padrão = "netqos"
Nível de log	número inteiro (de 1 a 5)	0 -Desativado, 1 - grave, 2 - erro, 3 - aviso, 4 - informações, 5 - depuração
Tamanho do arquivo de log (MB)	número inteiro (de 1 a 1000)	

Configurar o coletor do Flow Analysis

Os atributos a seguir para o probe do Flow Analysis são definidos usando a guia **Configurações do Coletor** a partir da interface gráfica do usuário de configuração do Flow Analysis.

Siga estas etapas:

1. Digite um nome de usuário e senha do administrador DSA para permitir ao coletor do Flow Analysis autenticar no sistema do coletor. Isso é para que ele tenha acesso ao compartilhamento do coletor.

   Observação importante: o nome de usuário do administrador DSA é um nome de usuário do Windows que tem privilégios administrativos no sistema do coletor. Se o sistema do coletor foi configurado por alguém mais além de você, verifique com o administrador do servidor o nome de usuário do administrador DSA que foi configurado manualmente durante a instalação do coletor do Flow Analysis.

2. Digite o Destino da interceptação, que é o endereço IP do robô que controla os probes do Flow Analysis e snmptd no sistema do coletor.

3. Modifique, se desejado, a diferença de horário em segundos (o padrão é 180 segundos). Usando esse atraso, consultas feitas ao banco de dados ocorrem em um curto período de tempo após o início de um novo intervalo de dados, evitando problemas de sincronização causado por latência de banco de dados. Em geral, quanto mais rápida o sistema do coletor for, menor esse intervalo pode ser, e vice-versa.

4. Reinicialize o sistema do coletor para instanciar essas alterações.

Observação: as alterações feitas aqui são aplicadas para o coletor que está atualmente selecionado na barra superior do menu da interface de usuário de relatórios do Flow Analysis.

Atributo	Tipo	Observações
Nome de usuário do administrador DSA	Endereço IP \ sequência de caracteres	exemplo: 172.19.0.24 \ nqadmin (padrão)
Senha do administrador do DSA	sequência de caracteres	exemplo: "nq" (padrão)

Destino de interceptação do SNMP	Endereço IP	IP do snmptd (robô)
Diferença de tempo em segundos	inteiro> 0	padrão = 180

Perfis de instalação do SNMP

Ao clicar em **Todos os roteadores** no quadro esquerdo, a tela **Perfil de SNMP** é exibida no quadro direito:

Clicando no item de menu **Novo** no Perfil de SNMP, ou clicando e selecionando um perfil existente a interface do usuário de configuração do **perfil de SNMP** é exibida à direita. Defina os seguintes atributos usando esta GUI:

Atributo	Tipo	Observações
Ativo	boolean	se o perfil é usado ou não para o dispositivo selecionado; ativo é o padrão
Ativado	boolean	se o perfil é usado ao tentar se comunicar com um dispositivo selecionado; ativo é o padrão
Classificação do perfil	integer	ordem na qual o perfil foi tentado/comparado em relação a um roteador; números mais baixos indicam precedência na ordem
Porta de gerenciamento	integer	padrão = 161
Descrição	sequência de caracteres	
Versão do SNMP	SNMP v1, v2 ou	Definir a cadeia de caracteres da comunidade para SNMP v1 e v2

	v3	Para o SNMP v3, defina: tipo de segurança, chave de autenticação, protocolo de autenticação (nenhum, MD5, SHA), Nome de usuário, chave de privacidade, Protocolo de privacidade (nenhum, DES, AES e DES triplo)

Configurar Interfaces

Clicar em um dispositivo de rede listado no quadro esquerdo exibe as **Interfaces** que estão disponíveis no dispositivo de rede selecionado:

Interfaces

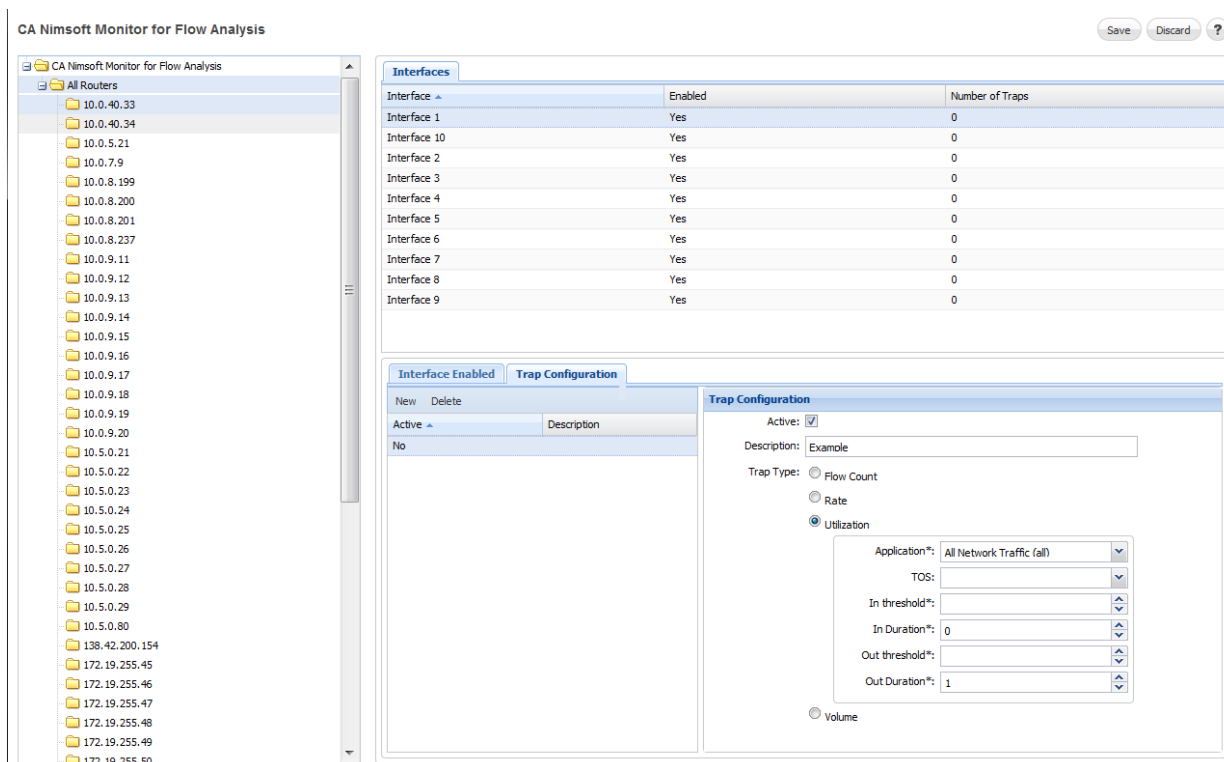
Interface	Interface Description	Interface Alias	Agent Type	Interface Type	Enabled	Interface Speed	Number of Traps
Interface 1	Interface 1		WAN	other	Yes	Unknown	0
Interface 10	Interface 10		WAN	other	Yes	Unknown	0
Interface 2	Interface 2		WAN	other	Yes	Unknown	0
Interface 3	Interface 3		WAN	other	Yes	Unknown	0
Interface 4	Interface 4		WAN	other	Yes	Unknown	0
Interface 5	Interface 5		WAN	other	Yes	Unknown	0
Interface 6	Interface 6		WAN	other	Yes	Unknown	0
Interface 7	Interface 7		WAN	other	Yes	Unknown	0
Interface 8	Interface 8		WAN	other	Yes	Unknown	0
Interface 9	Interface 9		WAN	other	Yes	Unknown	0

Clicar em uma interface exibe a interface do usuário de configuração da **Interface ativa** abaixo:

Atributo	**Tipo**	**Observações**
Ativado	boolean	se a interface está sendo monitorada ou não para dados do NetFlow; default=enabled

Configurar interceptações

Clicar em **Configuração de Interceptação** exibe uma lista de interceptações definidas na interface específica do dispositivo de rede selecionado:

Clicar em uma configuração de interceptação na lista exibe a GUI de **Configuração de interceptação** à direita:

Todos os tipos de interceptação compartilham dois atributos -- Ativo e Descrição.

Atributo	Tipo	Observações
Ativo	boolean	se uma interceptação SNMP for emitida ou não para a configuração especificada e interface atribuída; padrão=ativo
Descrição	sequência de caracteres	

Cada tipo de interceptação oferece atributos de configuração adicionais específicos aos seus objetivos:

Contagem de fluxo

Taxa

Utilização

Volume

Configurar relatórios

Depois que as etapas de configuração anteriores são realizadas, você estará pronto para visualizar os relatórios do Flow Analysis.

Consulte a seção sobre Relatórios (na página 27) para obter uma descrição sobre como configurar e usar os relatórios do Flow Analysis e as opções que estão disponíveis.

Capítulo 3: Relatórios

Relatórios de dados do Flow Analysis

A interface web do Flow Analysis oferece uma visão integrada dos aplicativos N principais, os hosts e interfaces de dispositivos da rede. Esta seção descreve os tipos de relatórios e as opções que estão disponíveis.

O Flow Analysis oferece uma exibição multidimensional do fluxo de dados recebidos da infraestrutura da sua rede. É possível passar os dados para responder a esses e outros tipos de perguntas:

- Quem conversou com quem? Quando? (Otimização da alocação da largura de banda e economia de custos ou detectar o tráfego mal-intencionado)
- Qual protocolo é mais intensamente usado? (Ofertas de classe de otimização de serviços)
- Onde está o maior volume de tráfego de rede? (Otimizar as configurações de VPN e alocação de largura de banda; solucionar problemas de alterações repentinas no uso)
- Que tipo de serviço (por exemplo, platina, ouro ou prata) está sendo afetado?

Usar a geração de relatórios de fluxo de dados juntamente com os relatórios de dados do QoS no UMP, é possível visualizar seu ambiente de serviço de TI a partir de uma perspectiva especifica a um dispositivo, serviço ou aplicativo.

Elementos comuns

Os seguintes elementos de GUI estão disponíveis em todos os relatórios do porlet do Flow Analysis:

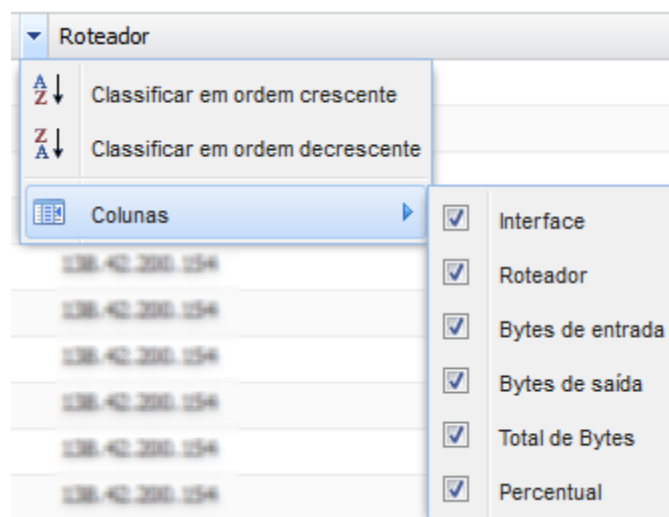
Elementos da barra superior

1. Hora -- o intervalo de tempo no qual os dados exibidos foram reunidos (últimos 15 minutos (padrão), última 1 hora, últimas 4 horas, último dia, última semana)
2. Principal -- número de interfaces/hosts/aplicativos mostrados nos relatórios dos N principais (5, 10 (padrão), 15, 20, 25)
3. Coletor de Flow Analysis -- o coletor que está fornecendo dados para os relatórios; também conhecido como o probe do Flow Analysis
4. Botão Atualizar -- consulta o banco de dados para os últimos intervalos de dados. Pode ser definido como: manual e atualização automática (intervalos de 1, 5, 10 e 15 minutos)
5. Botão Configurar -- abre o painel de Configuração
6. Botão Ajuda -- exibe a ajuda online

Opções de gráfico

1. Gráfico de coluna
2. Gráfico de barras
3. Gráfico de linhas
4. Exportar para o CSV. Clique no ícone e digite um local de salvamento. Os dados exibidos no relatório é o que é salvo.

Opções de exibição da coluna

Clicar em um cabeçalho de coluna alterna os dados abaixo na ordem de classificação crescente ou decrescente. É possível ocultar ou exibir colunas usando as caixas de seleção.

Arrastar colunas

É possível arrastar colunas inteiras em uma ordem de preferência. Este reordenamento de coluna não é persistente se você atualizar ou fechar o navegador.

Detalhar links

Clique nos links em azul para as interfaces, hosts, conversas e outros itens. Cada exibição do UMP é um "URL de alto grau" o qual, se for copiado e colado em outra janela do navegador ou guia. exibirá a mesma página/relatório da web, com dados atualizados de acordo com o intervalo de tempo mais recente.

Exibir dicas de ferramentas

Exibe informações detalhadas para alguns itens em exibições de relatório ao posicionar o cursor sobre o item. Quando você passa o cursor sobre o gráfico de barras de dados você obtém uma dica de ferramenta e os dados correspondentes na tabela são realçados. Inversamente, ao passar o mouse sobre uma linha de dados em uma tabela destaca o gráfico de barra correspondente.

Sequência de caracteres de informação

Abaixo de cada relatório gráfico na parte inferior direita existe uma legenda que fornece detalhes sobre os dados exibidos no relatório.

Janela principal

A janela principal do Flow Analysis (ilustrado no exemplo a seguir) mostra os N principais dados para o fluxo de dados entre:

- Interfaces principais
- Hosts principais
- Aplicativos principais (protocolos)

Clicar em um nome de interface nas interfaces principais gráficas exibirá um relatório de detalhamento sobre os N principais comunicações/hosts/aplicativos a partir da perspectiva daquela interface.

Da mesma forma, se você clicar em um nome de host ou aplicativo em seus respectivos gráficos detalhará o host ou aplicativo e fornecerá informações adicionais.

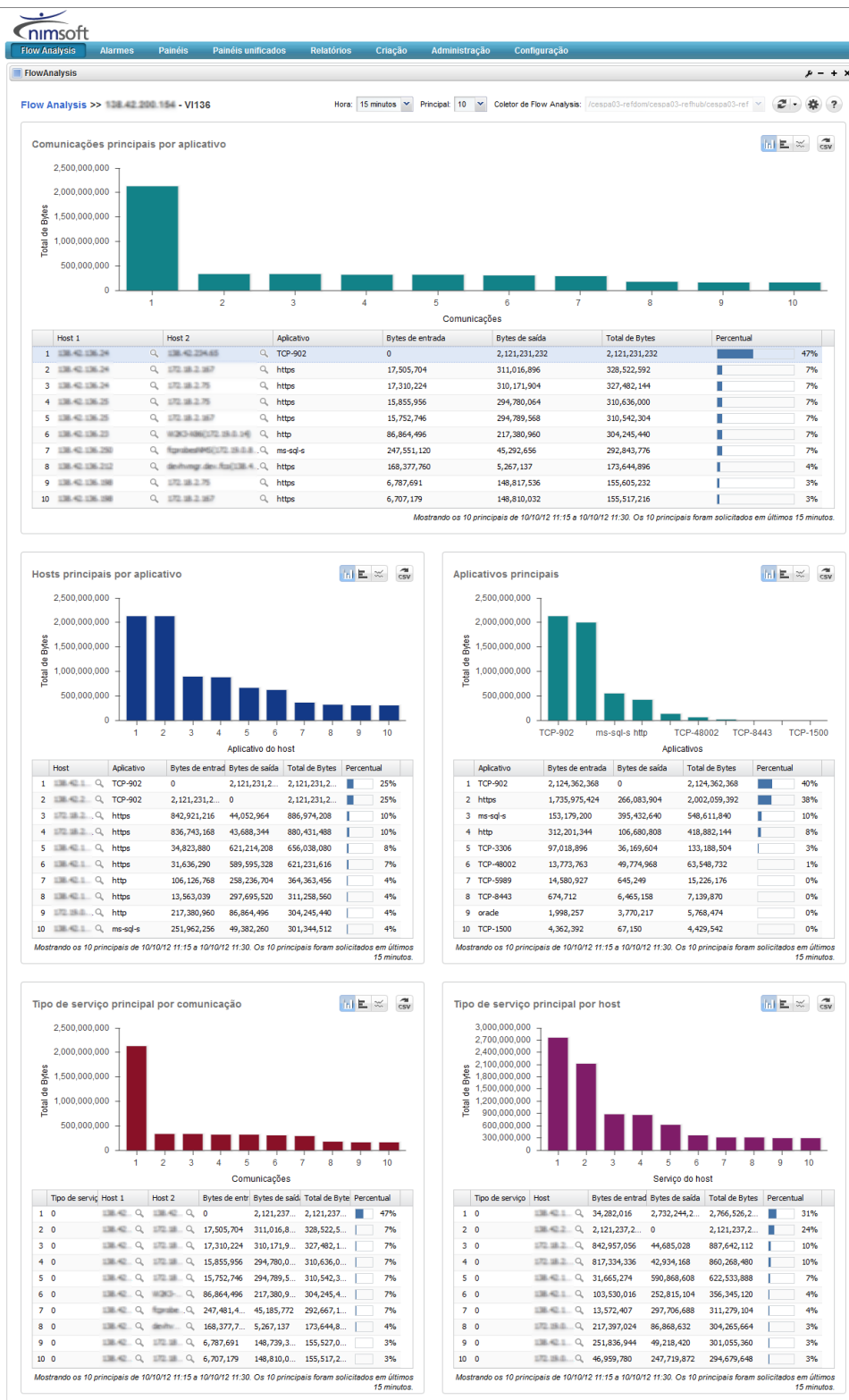
Clicar no link do USM para pesquisar o dispositivo no Unified Service Manager (dependendo do dispositivo, nem todas as pesquisas fornecerão informações adicionais):

nimsoft
Flow Analysis
Alarmes
Painéis
Painéis unificados
Relatórios
Criação
Administração
Configuração
FlowAnalysis
Flow Analysis
Hora: 15 minutos
Principal: 10
Coletor de Flow Analysis: /cespa03-refdom/cespa03-refhub/cespa03-ref
Interfaces principais
Interface | Roteador | Bytes de entrada | Bytes de saída | Total de Bytes | Percentual
1 Vl136 1,790,827,648 300,442,112 2,091,269,760 33%
2 Vl301 89,869,128 1,674,383,232 1,764,252,416 28%
3 Vl229 1,098,180,864 86,834,128 1,185,015,040 19%
4 Vl303 48,666,256 553,453,760 602,120,000 9%
5 Vl300 0 441,215,424 441,215,424 7%
6 Vl135 106,032,136 8,171,279 114,203,416 2%
7 Vl313 3,201,143 90,763,776 93,964,920 1%
8 Vl316 41,437,080 2,963,121 44,400,200 1%
9 Vl311 8,373,562 13,624,478 21,998,040 0%
10 Vl310 9,040,737 6,697,340 15,738,077 0%
Mostrando os 10 principais de 10/10/12 11:00 a 10/10/12 11:15. Os 10 principais foram solicitados em últimos 15 minutos.
Hosts principais
Total de Bytes
Hosts
Host | Bytes de entrada | Bytes de saída | Total de Bytes | Percentual
1 61,367,868 1,055,067,456 1,116,435,328 21%
2 835,121,856 43,451,864 878,573,696 16%
3 833,526,336 43,582,948 877,109,312 16%
4 34,542,360 619,566,400 654,108,736 12%
5 31,758,532 590,241,600 622,000,128 11%
6 408,043,520 0 408,043,520 8%
7 13,473,717 297,776,928 311,250,656 6%
8 185,965,280 15,702,758 201,668,032 4%
9 171,569,792 5,591,571 177,161,360 3%
10 159,877,248 10,060,237 169,937,488 3%
Mostrando os 10 principais de 10/10/12 11:00 a 10/10/12 11:15. Os 10 principais foram solicitados em últimos 15 minutos.
Aplicativos principais
Total de Bytes
https
http
TCP-8443
TCP-5989
ms-sql-s
dns
Aplicativos
Aplicativo | Total de Bytes | Percentual
1 https 2,981,445,888 94%
2 http 67,846,984 2%
3 TCP-3306 19,418,862 1%
4 TCP-8443 19,075,416 1%
5 TCP-39903 15,943,188 1%
6 TCP-5989 14,030,757 0%
7 TCP-48001 13,237,759 0%
8 ms-sql-s 12,928,050 0%
9 TCP-3203 6,348,722 0%
10 dns 6,254,229 0%
Mostrando os 10 principais de 10/10/12 11:00 a 10/10/12 11:15. Os 10 principais foram solicitados em últimos 15 minutos.

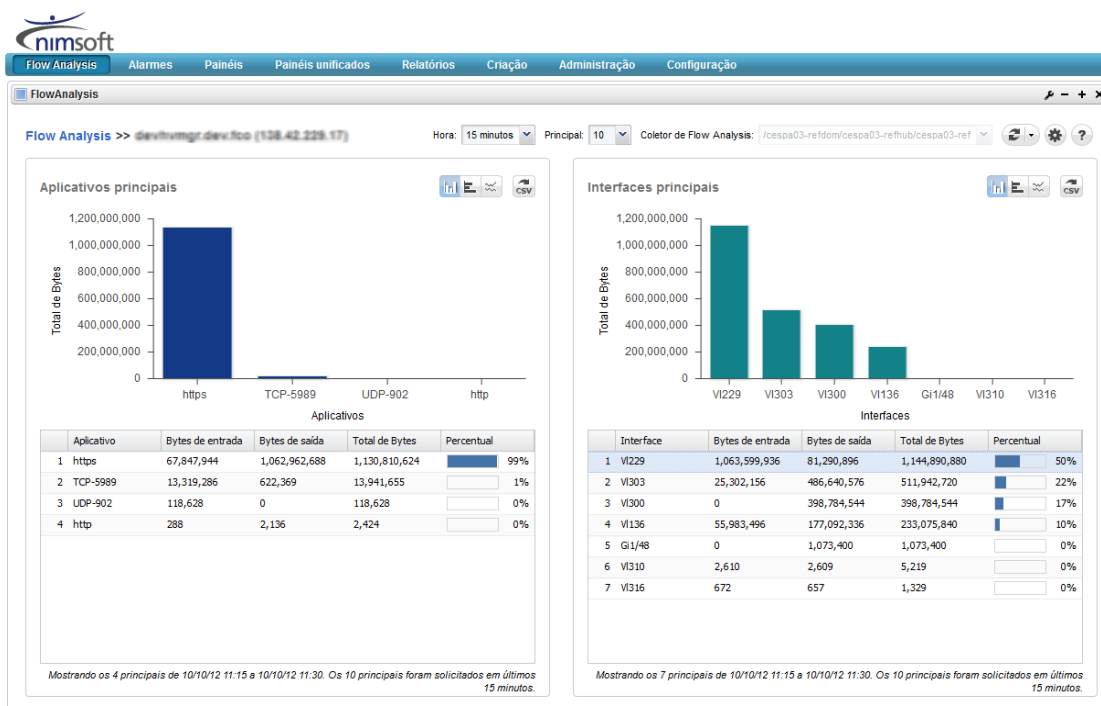
Interfaces

No relatório principal, fazer uma busca detalhada em uma interface mostra o tráfego que está fluindo através da interface do dispositivo de rede selecionado. Estes relatórios são exibidos:

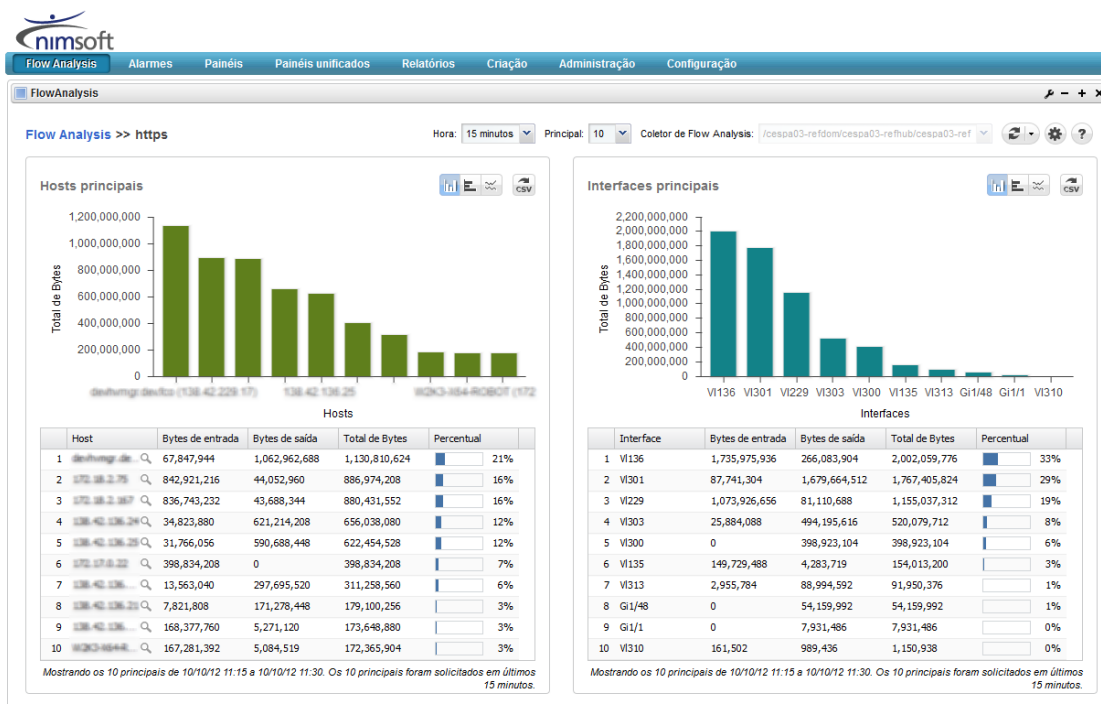
- Comunicações principais por aplicativo
- Hosts principais por aplicativo
- Aplicativos principais
- Tipo de serviço principal por comunicação
- Tipo de serviço principal por host

Essas informações são úteis para otimizar as configurações de VPN e alocação de largura de banda, ajuste fino das opções de serviço, ou solução de problemas de mudanças inesperadas no uso. Elas podem ser usadas para otimizar alocações de largura de banda ou para detectar o tráfego mal-intencionado.

Hosts

Na exibição principal, fazer uma busca detalhada em um host fornece dois relatórios sobre o tráfego visto naquele host:

- Aplicativos principais
- Interfaces principais

Aplicativo

Fazer uma busca detalhada em um aplicativo a partir da tela principal exibe, dependendo do protocolo, até dois relatórios detalhados:

- Hosts principais
- Interfaces principais

Capítulo 4: Solução de problemas

Sem dados exibidos em relatórios (Tempo de atraso nos dados relatados)

Válido em todas as plataformas

Sintoma: exibição contínua dessa mensagem de erro:

Nenhum dado retornado

Talvez não haja dados no período especificado. Se você espera ver os dados no intervalo especificado, tente as seguintes sugestões:

- Clique aqui para recuperar.
- Verifique o status do monitoring_services.
- Verifique se o probe de flow para o coletor de Flow Analysis"/cespa03-refdom/cespa03-refhub/cespa03-ref" está em execução e funcionando corretamente.

Detalhes:
Código do status de HTTP: 204 No Content

Solução: configure a configuração da diferença de tempo na guia Configurações do coletor

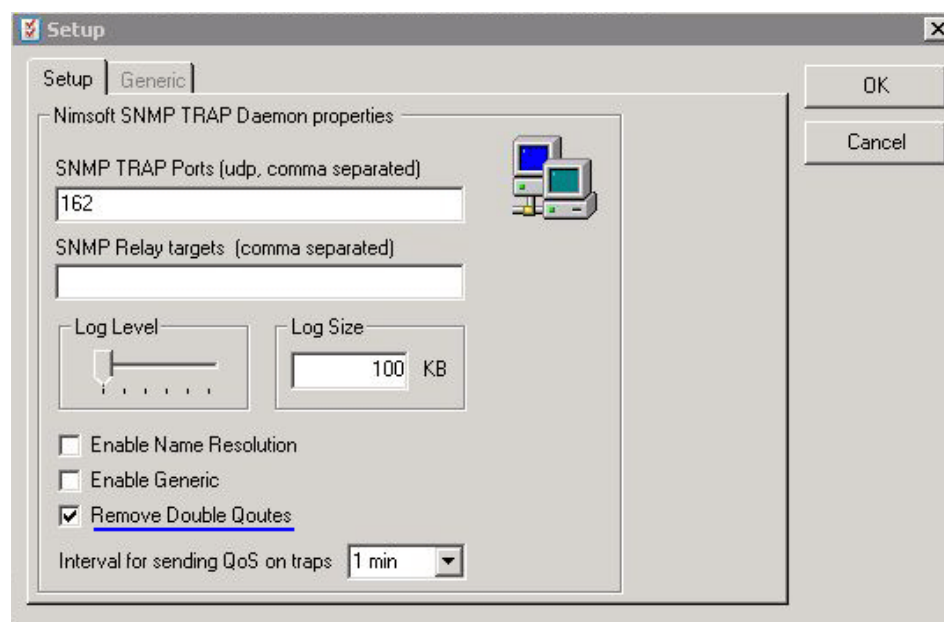
Configuração da **Diferença de tempo em segundos** para um valor maior pode ser necessária para sistemas de coletor do Flow Analysis lentos.

Links para USM não tem função

Válido em todas as plataformas

Sintoma: ao clicar no ícone de ampliação "Pesquisar USM" na GUI do Flow Analysis, o sistema informa "Sem Métricas disponíveis". Isso acontece para todos os dispositivos procurados no USM.

Solução: certifique-se que o probe snmptd está configurado corretamente, usando o seguinte método:

Na configuração do probe snmptd (clique duas vezes no ícone do probe snmptd no Gerenciador de infraestrutura), certifique-se de que a caixa de seleção "Remover as aspas duplas" está marcada.

Link para o USM Exibe dispositivo incorreto

Válido em todas as plataformas

Sintoma: ao clicar no ícone de ampliação "Pesquisar USM" na GUI do Flow Analysis, conecta a um dispositivo incorreto na exibição do USM.

Motivo: se um dispositivo não está configurado como parte de um grupo do USM, o algoritmo de busca do USM não será capaz de fazer a correspondência exata e retornará a correspondência mais próxima que encontrar.

Solução: verifique no UMP se o dispositivo está configurado em um grupo. Se ele não estiver em um grupo, adicione-o a um grupo existente ou crie um novo grupo e adicione-o a este grupo.

Coletor não mostrados no menu suspenso

Válido em todas as plataformas

Sintoma: ao clicar na barra superior do menu suspenso para mostrar coletores disponíveis, nenhum é exibido, ou aquele desejado não está listado.

Motivo: o serviço de detecção não encontrou o probe coletor no sistema do coletor.

Solução: pare e reinicie os probes Discovery_server e Discovery_agent no Gerenciador de infraestrutura.

Interface denominada Null0 ou Nu0

Válido em todas as plataformas

Sintoma: uma das interfaces TopN é exibida com um nome em branco.

Motivo: o comportamento do dispositivo Cisco padrão é atribuir dados de fluxo para tráfego errado no dispositivo para uma interface de simulação denominada "Null0" ou "Nu0". Se a interface Nu0 em um roteador aparece em um relatório de fluxo, o nome da interface está sendo mostrado atualmente como em branco.

Solução: nenhuma, este é o comportamento esperado.

Código de mensagem de erro 500

Sintoma: obter o código de erro 500

Causa: os serviços de monitoramento não podem localizar todos os probes. Isso pode significar que o discovery_server não está em execução. Mesmo que o próprio probe não está sendo executado e aparecerá (marcado em laranja/vermelho) na lista de detecção.

Código de mensagem de erro 400

Sintoma: obter o código de erro 400

Causa: não é possível se comunicar com o probe. Isso ocorre quando o probe não está sendo executado ou não é possível se comunicar com ele.

Código de mensagem de erro 200

Sintoma: obter o código de erro 200

Causa: o probe responde com um conjunto de dados vazio. Isso pode acontecer se não houver nenhum dado disponível para o intervalo de tempo selecionado ou se a hora do sistema definida na caixa NetQoS está incorreta.